使用Expressway x15.5导航客户端EKU日落

简介

本文档介绍使用Cisco Expressway x15.5导航客户端EKU日落。

背景信息

数字证书是由受信任的证书颁发机构(CA)颁发的电子凭证，通过确保身份验证、数据完整性和机密性来保护服务器和客户端之间的通信。这些证书包含定义其用途的扩展密钥使用(EKU)字段：

- 服务器身份验证EKU(id-kp-serverAuth)在服务器提供证书以证明身份时使用。
- 客户端身份验证EKU(id-kp-clientAuth)用于双向TLS(mTLS)连接，其中双方相互进行身份验证。

传统上，单个证书可以同时包含服务器和客户端身份验证EKU，使其具有双重用途。这对于在不同连接场景中同时充当服务器和客户端的产品（例如Cisco Expressway）尤为重要。

问题定义

Chrome根计划策略更改

自2026年6月起，Chrome根程序策略限制包含在Chrome根存储中的根证书颁发机构(CA)证书，逐步取消多用途根以调整所有公共密钥基础结构(PKI)层次结构以仅服务TLS服务器身份验证使用案例。

主要政策要求

- 公共根CA必须声明仅用于服务器身份验证(id-kp-serverAuth)的扩展密钥使用(EKU)。
- 禁止在这些证书中包含客户端身份验证EKU。
- 公共服务器TLS证书没有更多混合使用的根CA。
- 实施时间表：2026年6月

公共CA响应时间表

- 2025年10月默认情况下，许多公共CA(DigiCert、Sectigo、SSL)开始发布纯服务器证书。
- 2026年5月：公共CA服务器停止颁发客户端身份验证EKU认证
- 2026年6月：Chrome根计划策略完全生效

注意：此策略仅适用于公共CA颁发的证书。私有PKI和自签名证书不受此策略的影响。

如果您有兴趣阅读Expressway上客户端EKU的日落设置的影响，请参阅在公共CA证书中准备Expressway客户端身份验证EKU日落。

Expressway版本x15.5，带解决方案

Expressway x15.5

Expressway x15.5针对由于所有公共证书颁发机构对客户端EKU进行设置而引起的问题提供了建议的解决方案。这是一个全球性问题，影响选择使用公共PKI证书的所有供应商/部署。

x15.4（之前的版本）有一个CLI命令交换机，允许管理员在Expressway E上上传仅服务器EKU证书（不存在客户端EKU）。

xConfiguration XCP TLS Certificate CVS EnableServerEkuUpload:开启

注意：x15.5已弃用此命令。

X15.5证书存储增加

x15.5有两个证书存储区：

1.服务器证书存储

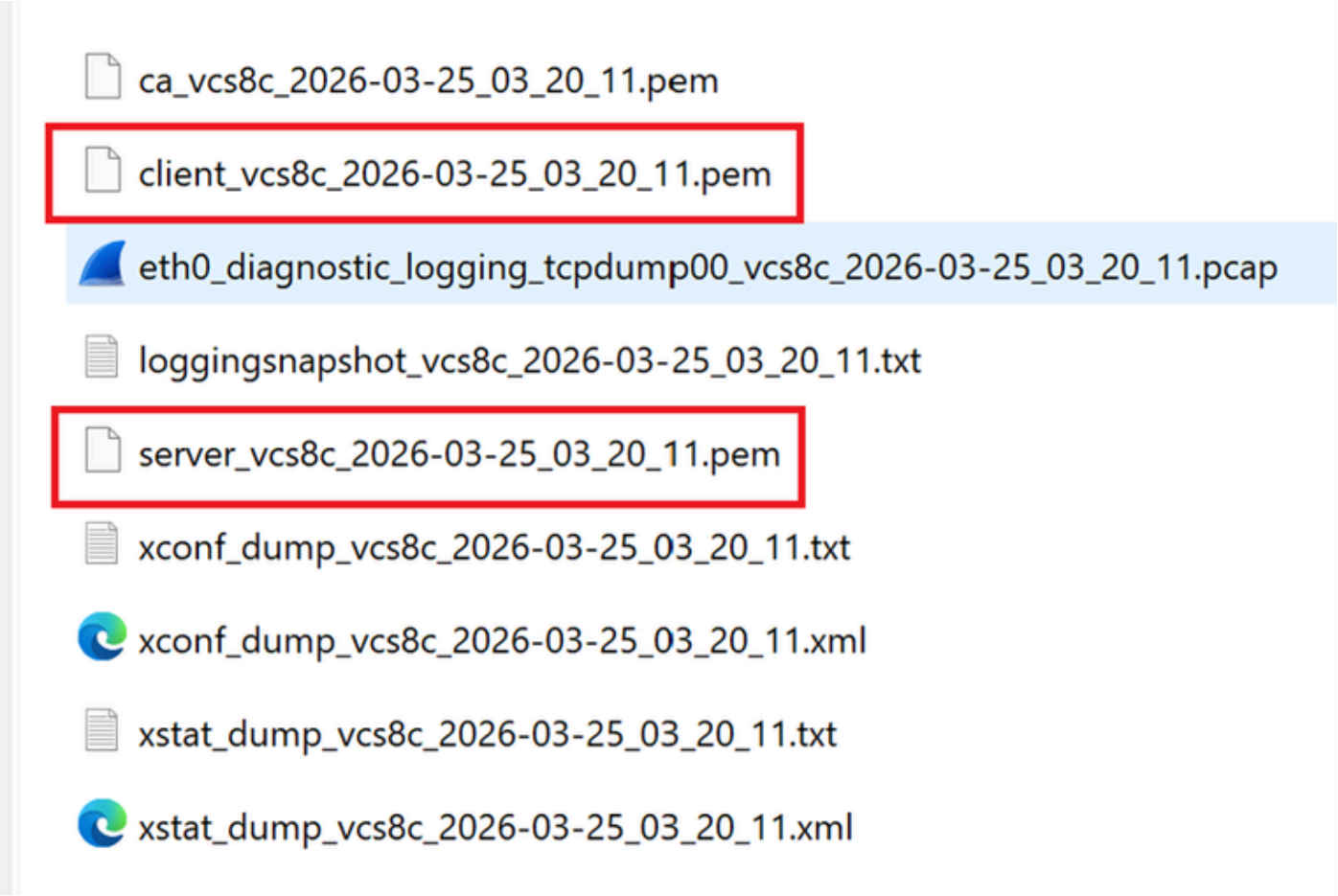
2.客户端证书存储

高速公路（单网卡或双网卡）：两个Expressway接口均可根据需要使用2个证书存储区。

示例：

- 当expressway在TLS握手期间充当客户端时，将显示客户端证书。
- 当expressway在TLS握手期间充当服务器时，将显示服务器证书。

注意：两个证书存储（客户端和服务器）使用相同的受信任CA库。确保已签名服务器和客户端证书的CA已正确上传到信任库中。 诊断日志现在包含PEM文件格式的服务器证书和客户端证书。



从X15.4或早期版本升级到X15.5

执行升级时，来自x15.4或早期版本的服务器证书会复制到x15.5上的客户端证书存储区。x15.5上的客户端证书存储区和服务器证书存储区具有相同的证书。

屏幕截图示例

15.4上的Expressway服务器，当前服务器证书序列号46:df:76:aa:00:00:00:00:29

证书:

版本：3(0x2)

序列号(S):

46:df:76:aa:00:00:00:00:00:29

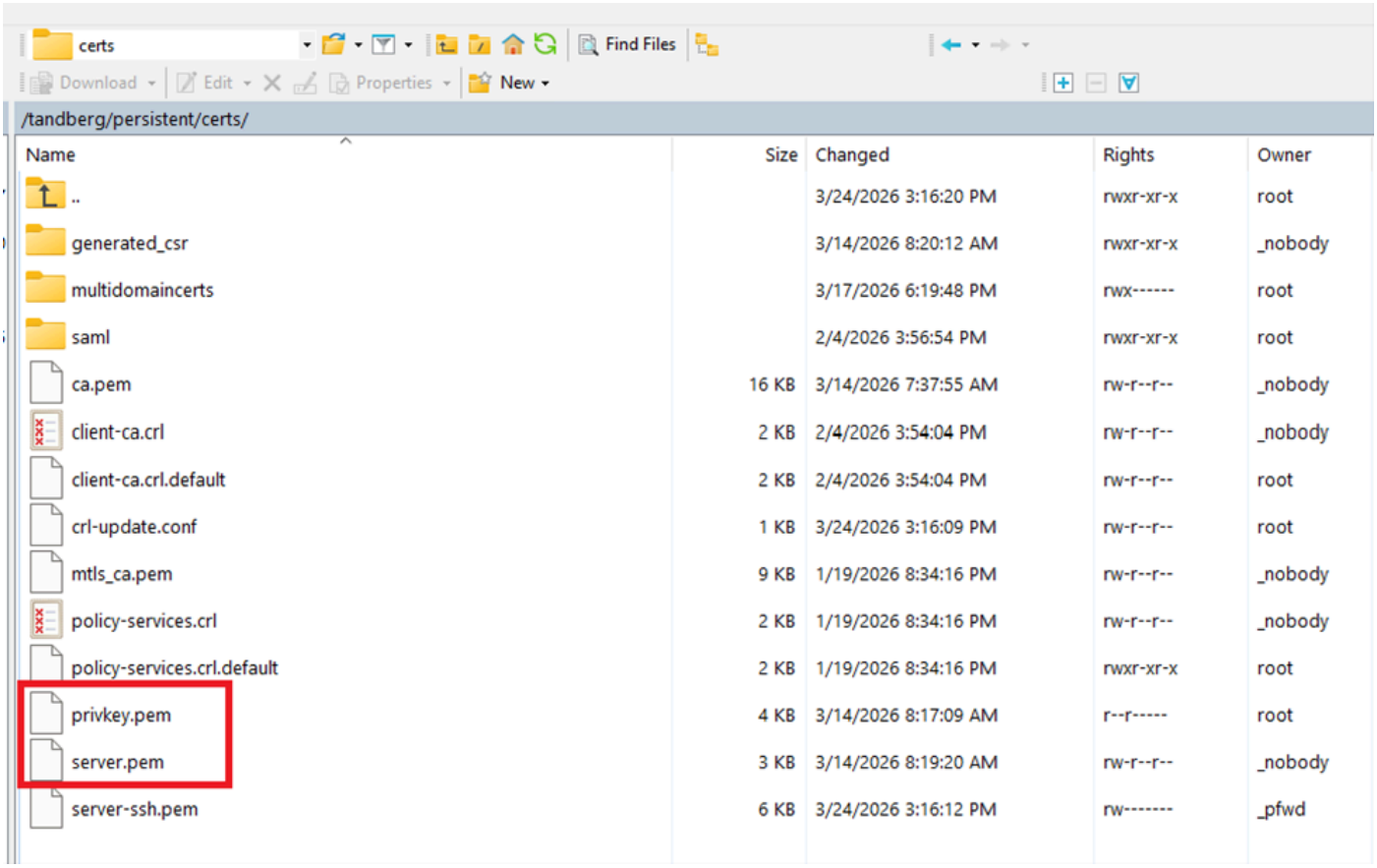
有效性

不早于：3月14日02:37:40 2026格林尼治标准时

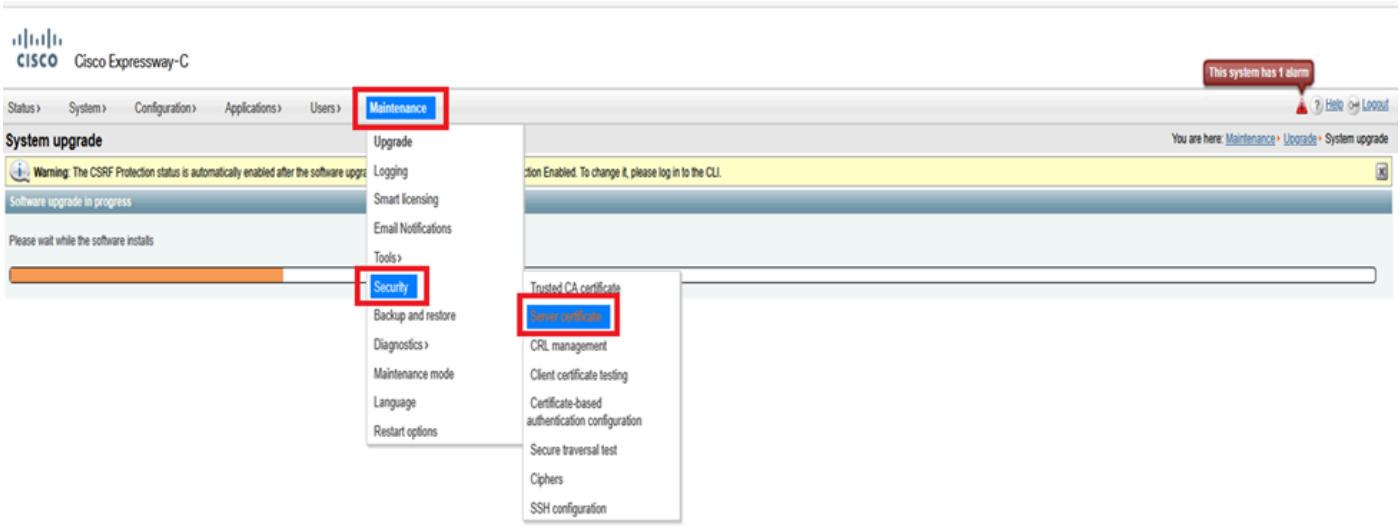
不晚于：3月14日02:47:40 2028格林尼治标准时

主题：C = IN、ST = KA、L = KA、O = Cisco、OU = TAc、CN = cluster.s.com

x15.4上的Expressway文件系统持久/证书目录：

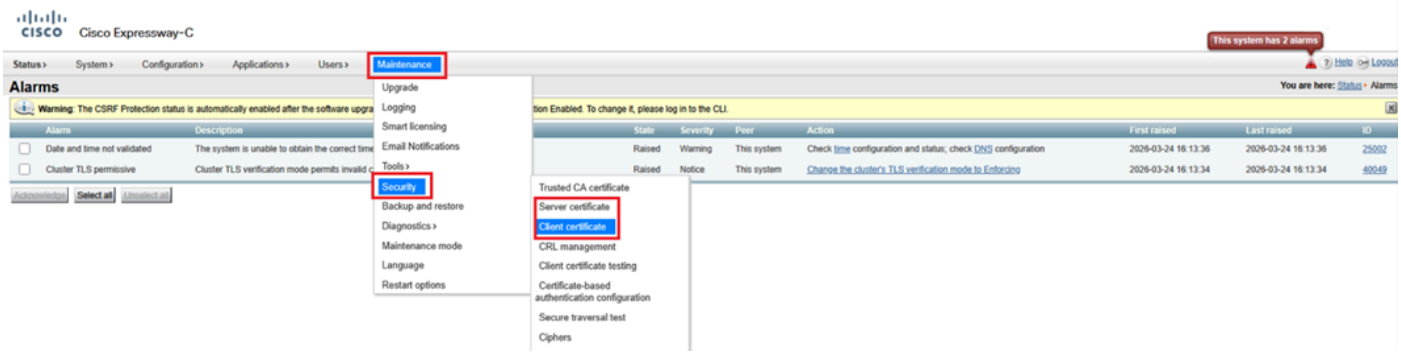


x15.4上的Expressway菜单(Maintenance > Security > Server certificate)（仅存在服务器证书字段）：



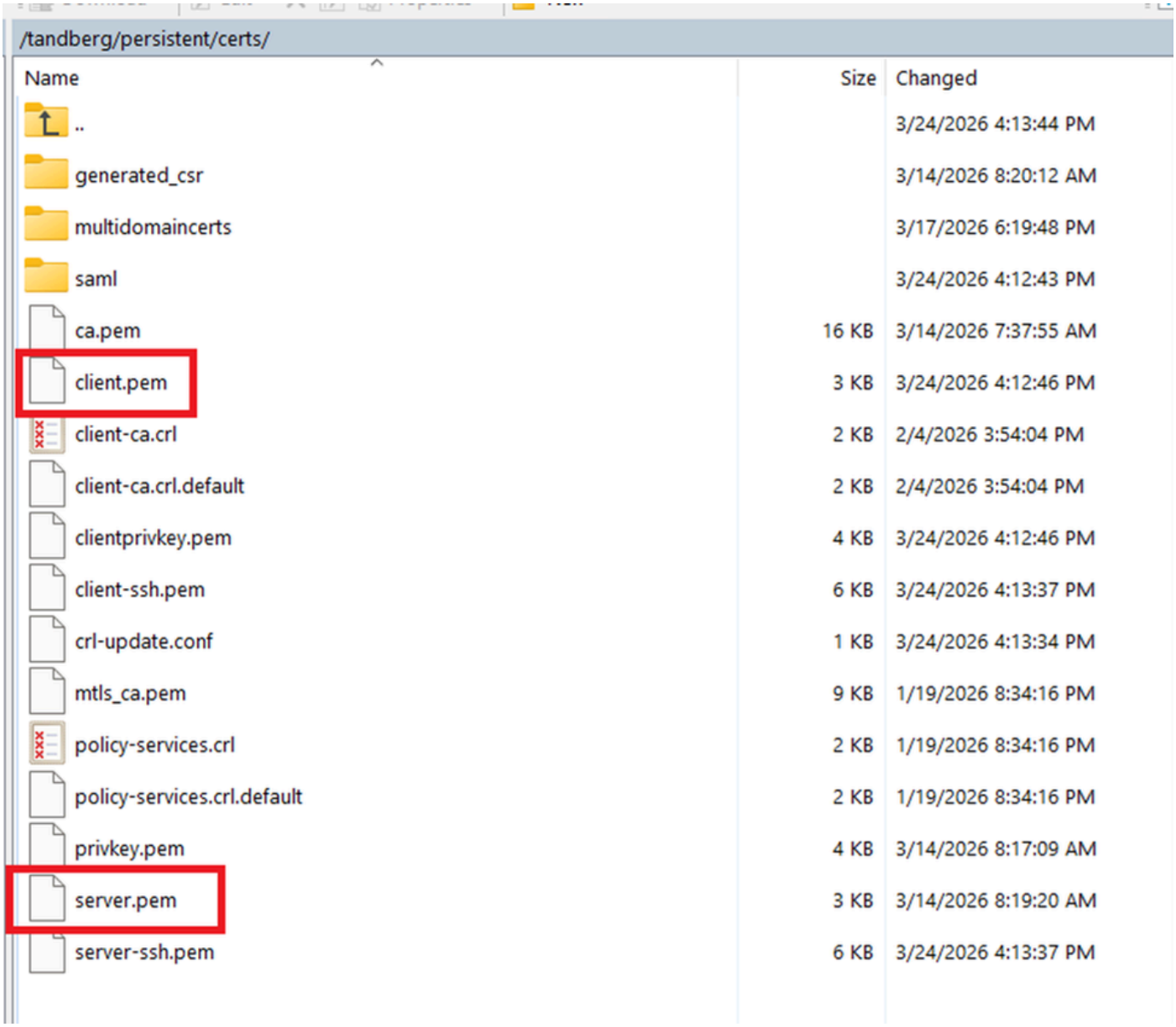
成功升级到x15.5后

此处，您在Maintenance > Security > client certificate和server certificates下看到两个证书选项。升级到x15.5后，Web管理员上的服务器和客户端证书门户显示相同的证书，因为来自x15.4的服务器证书已复制到x15.5上的客户端证书存储区。



升级到x15.5的现有证书和私钥已复制到客户端证书存储区。

x15.5上的Expressway文件系统持久/证书目录：



在TLS握手期间进行X15.5 EKU检查

在x15.5上，引入了一个新的CLI命令来检查TLS握手期间的扩展密钥使用(EKU)。默认值为“ON”。命令集在Expressway核心和边缘上有效。

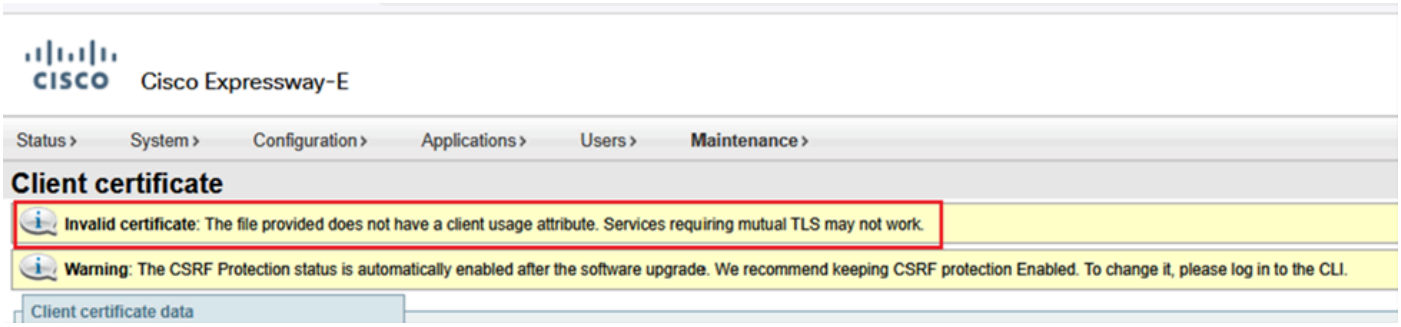
命令集触发检查所有到Expressway的入站SIP TLS连接。（提供入站客户端hello/证书）。 当打开“ON”时，这将检查TLS发起方提供的证书中是否包含客户端EKU。如果关闭，则绕过检查；但是，如果服务器EKU存在于证书中，则会对其进行检查。

xconfiguration SIP TLS Certificate ExtendedKeyUsage检查模式：开/关：

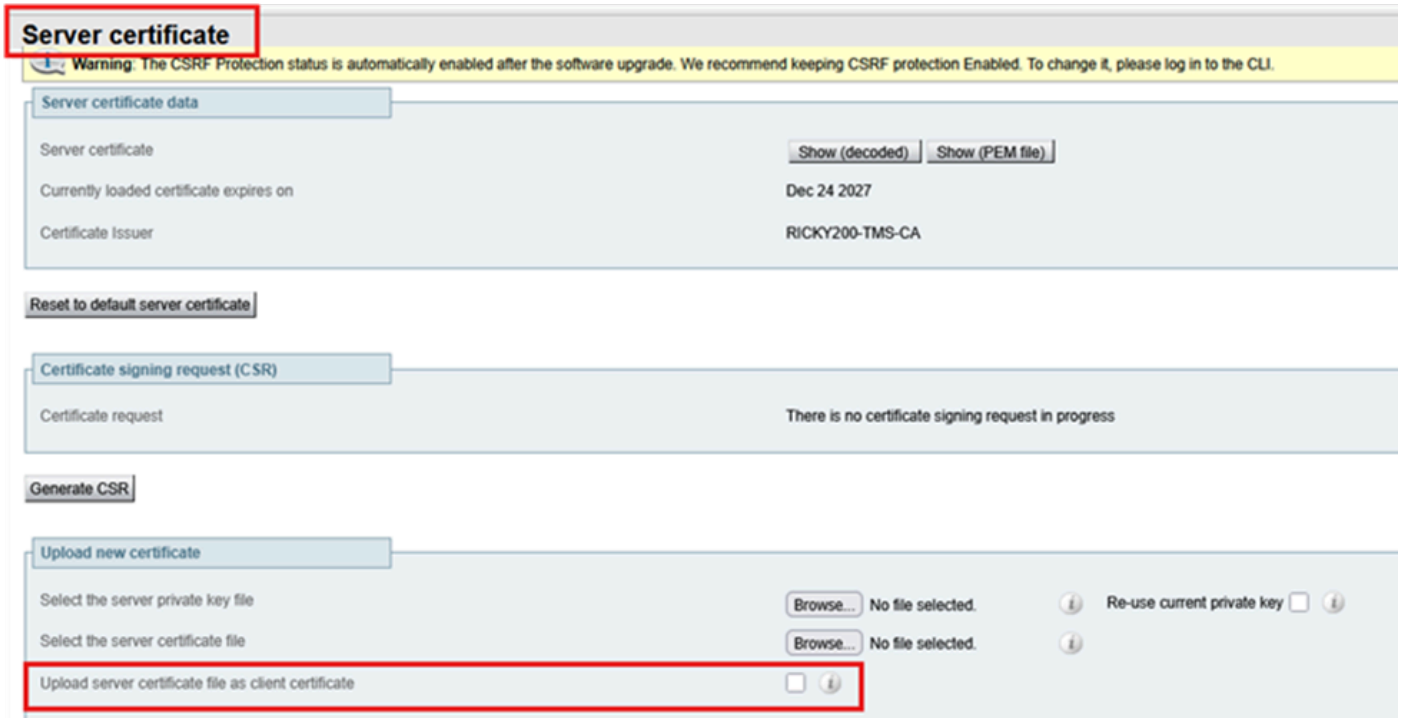
注意：如果生成客户端证书，对不包含客户端EKU的CSR进行签名（公共CA签名证书的示

例），则无法在客户端证书存储上手动上传此证书。因此，您需要确保通过签署CSR生成的证书始终包含客户端EKU（可以使用专用CA插入客户端EKU）。

提示：当您尝试从客户端证书存储上传CSR签名证书（缺少客户端EKU）时，此错误很明显。



但是，如果选择通过服务器证书存储上传仅具有服务器EKU（无客户端EKU）的证书，并选择上传服务器证书文件作为客户端证书，则证书将复制到客户端证书存储中。不想在Expressway-Edge上使用私有CA签名证书的管理员可以选择仅将服务器EKU从服务器证书存储复制到客户端证书存储。

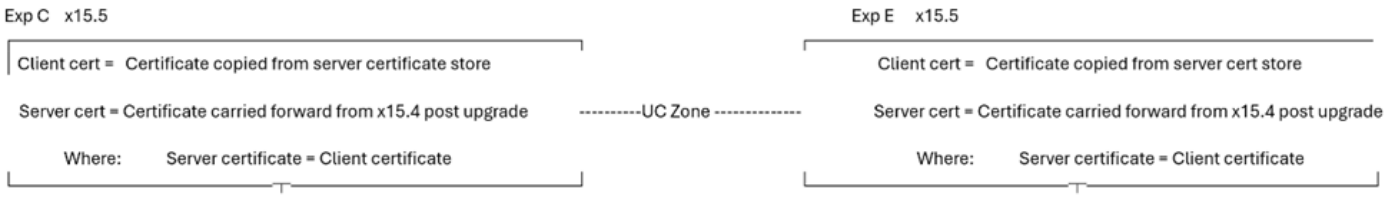


多个证书存储，多个部署方案

由于现在在Expressway上有两个证书存储，因此存在多个证书存储方案。

条件1:升级

当Expressway从x15.4或x15.5之前升级时，此情况为真。x15.4版本中的现有证书将复制到两(2)个证书存储中。在x15.5客户端和服务器上，证书相同。

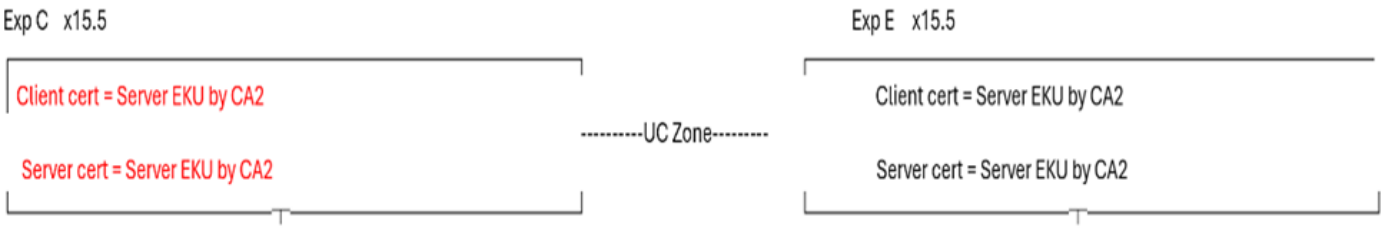


条件2:当管理员在x15.5上安装新证书（现有证书已过期）时

CA 1 =内部CA

CA 2 =公共CA

在接下来的图中，Expressway核心具有仅由CA 2（公共CA）签名的服务器EKU的客户端证书和仅由CA 2（公共CA）签名的服务器EKU的服务器证书。 同样，Expressway E具有由CA2（公共CA）签名的服务器EKU的客户端证书和仅由CA 2（公共CA）签名的服务器EKU的服务器证书。



如果Expressway核心服务器证书没有客户端EKU、统一通信穿越区域、MRA，则WebRTC代理不起作用。确保Expressway核心服务器证书具有客户端EKU。 这是用户选择对来自公共CA的所有证书进行签名的常见使用案例。由于公共CA在证书中不包括客户端EKU，统一通信穿越区域将变为活动状态。

要激活UC区域，一个快速修复方法是关闭Expressway E上的EKU检查。此时会显示UC区域。但是，SSH隧道保持非活动状态。从今天起，2222上的SSH隧道通信需要验证客户端EKU。

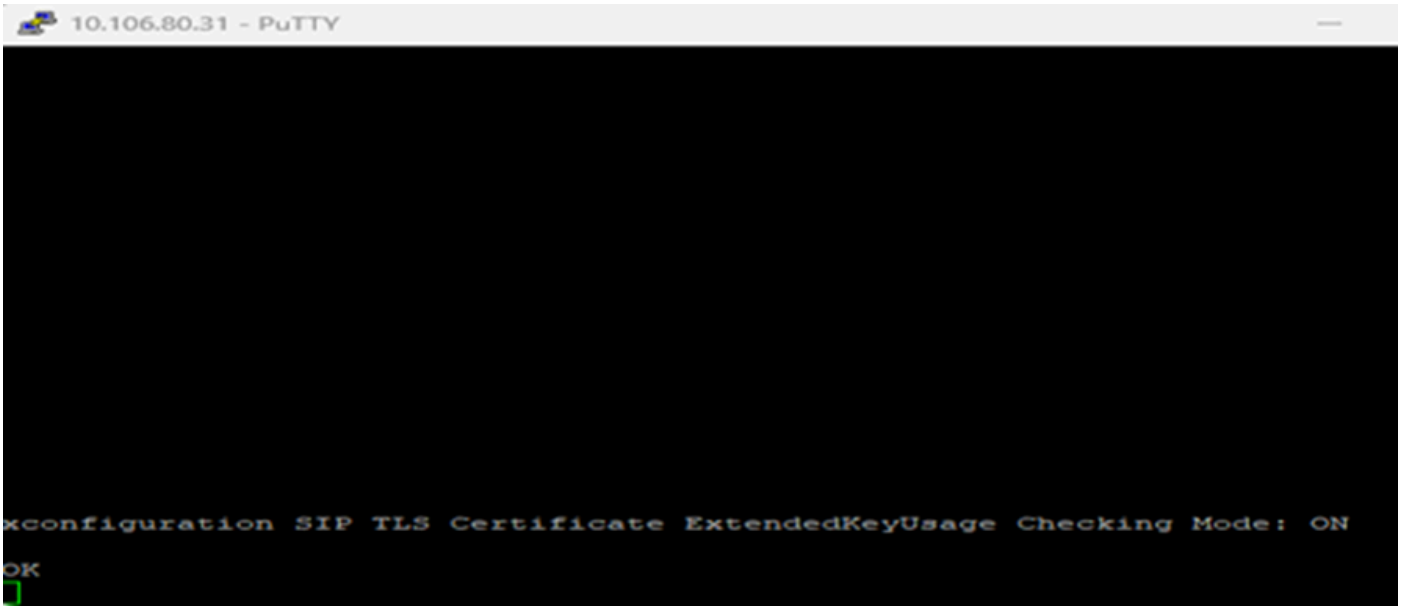
MRA客户端登录和WebRTC代理功能不起作用。您可能不得不使用私有CA。

测试案例1

- 当Expressway E上的EKU检查为“ON”时
- 当Expressway核心上的客户端和服务器证书仅具有服务器EKU时
- UC区域状态失败

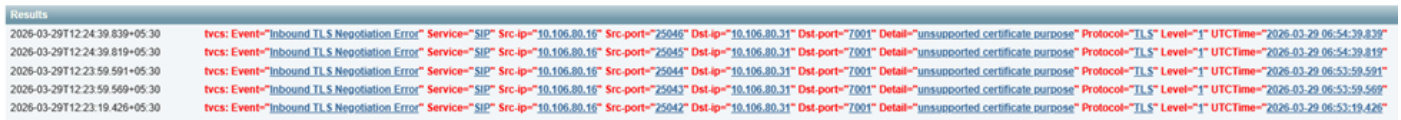
在Expressway-Edge ExtendedKeyUsage上检查。

xconfiguration SIP TLS Certificate ExtendedKeyUsage检查模式：开启:



统一通信区域故障：

Expressway E日志显示其中10.106.80.16 = Expressway核心，10.106.80.31 = Expressway边缘：

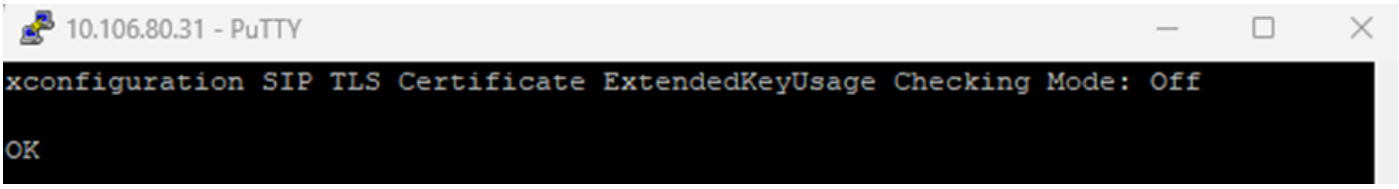


测试案例2

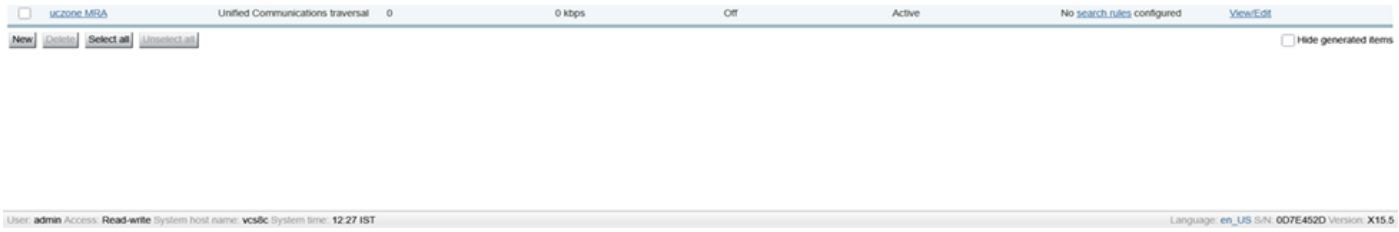
- 当Expressway E上的EKU检查处于关闭状态时
- 当Expressway核心上的客户端和服务器证书只有服务器时
- UC区域状态为ACTIVE

关闭Expressway E上的EKU检查。

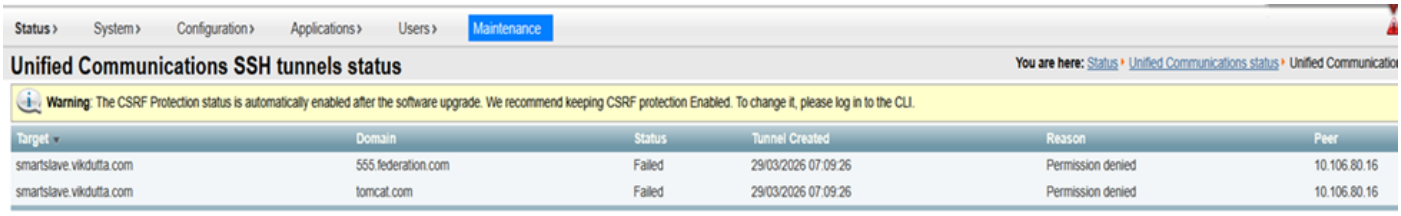
xconfiguration SIP TLS Certificate ExtendedKeyUsage检查模式：关闭



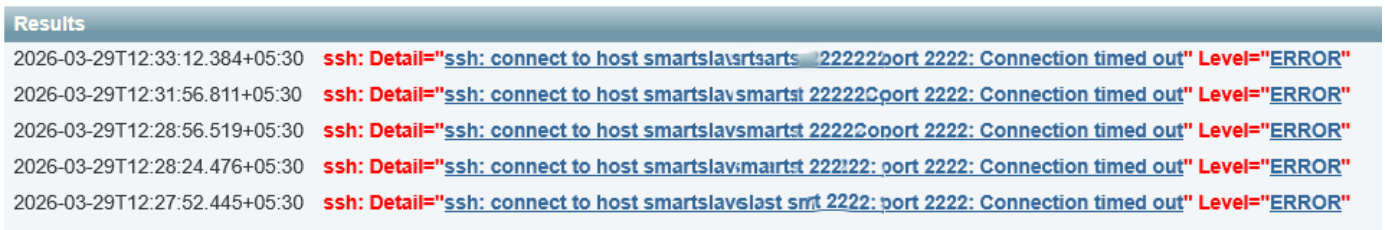
激活的统一通信区：



但是，ssh隧道仍然失败：



Expressway事件日志：

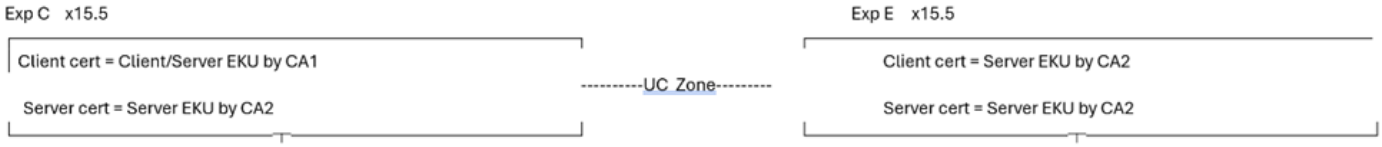


条件2.1:成功案例

CA 1 =内部CA

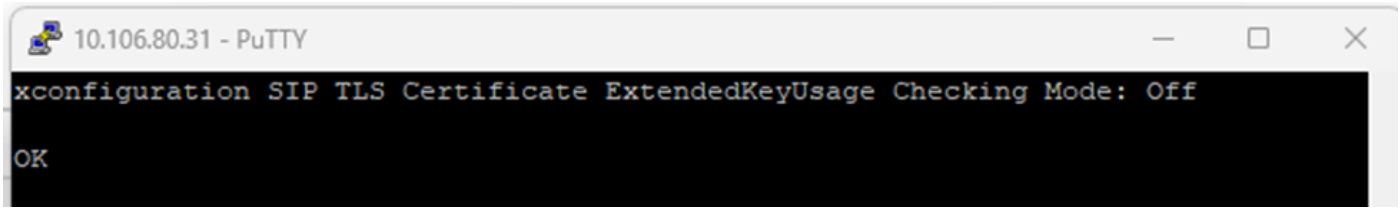
CA 2 =公共CA

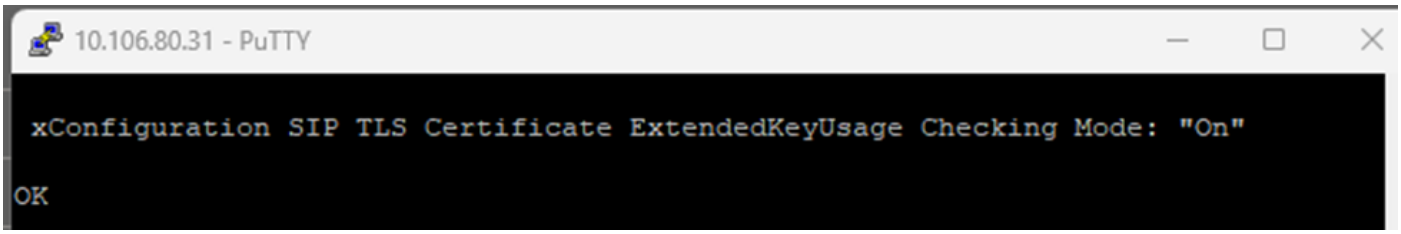
- 其中Expressway核心客户端证书由CA 1（内部CA）签名并包括，客户端/服务器EKU均包括。
- Expressway核心服务器证书由CA 2公共CA签署，仅包括服务器EKU。
- Expressway边缘服务器证书由CA 2公共CA签署，仅包括服务器EKU。
- Expressway边缘客户端证书由CA 2公共CA签署，仅包括服务器EKU。



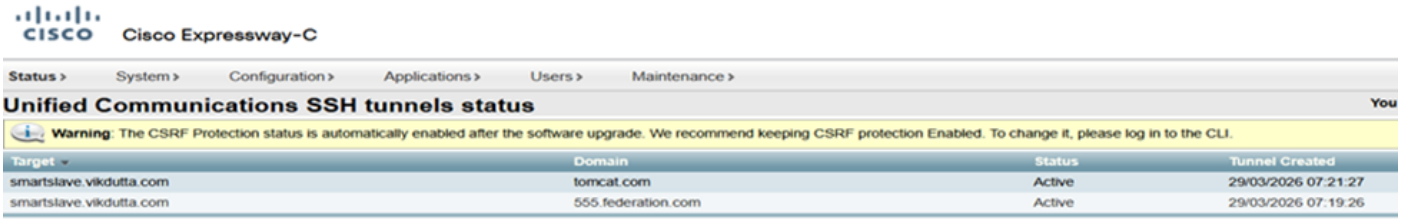
此条件是一个成功案例。 无论EKU检查模式是否为ON/OFF，统一通信区域和SSH隧道都会变为活动状态。MRA客户端工作。

Expressway边缘EKU检查是关闭还是打开并不重要。Expressway核心客户端证书包含客户端EKU:

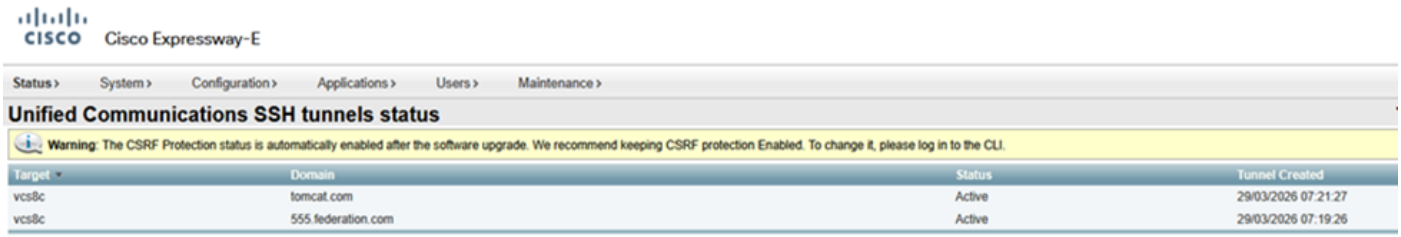




Expressway核心上的SSH隧道处于活动状态：

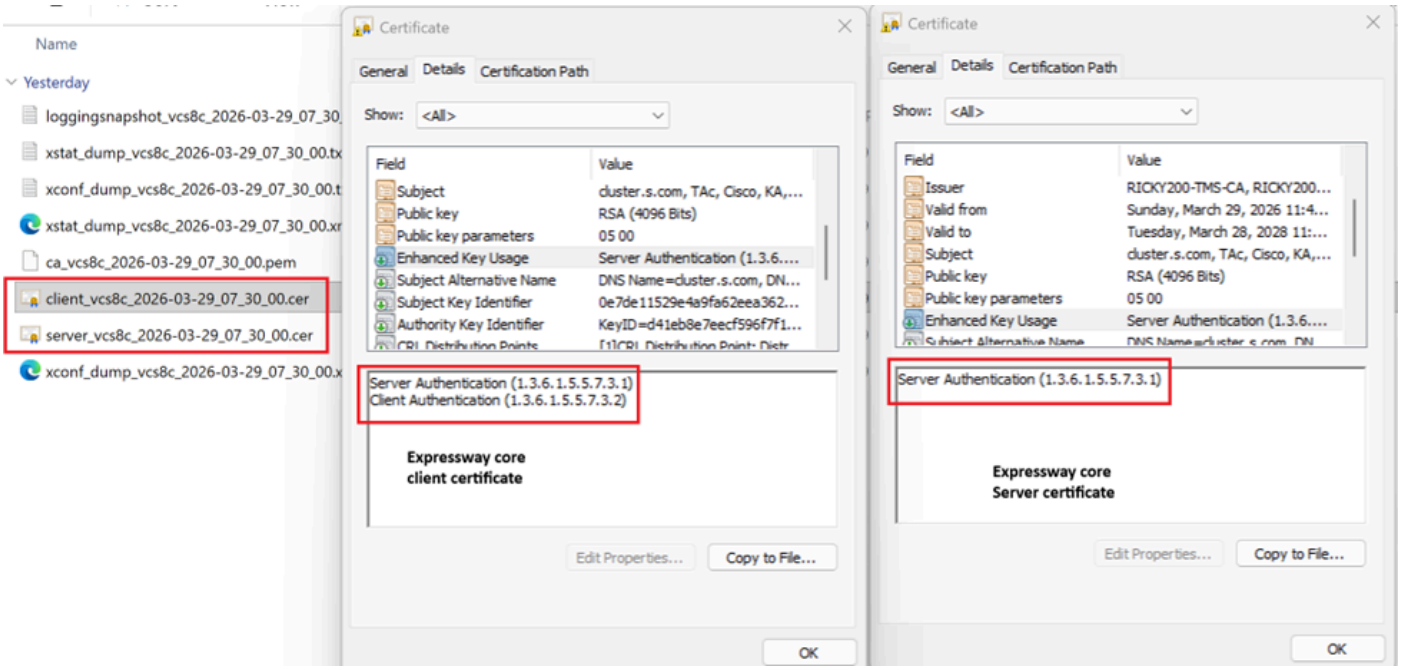


Expressway边缘上的SSH隧道处于活动状态：

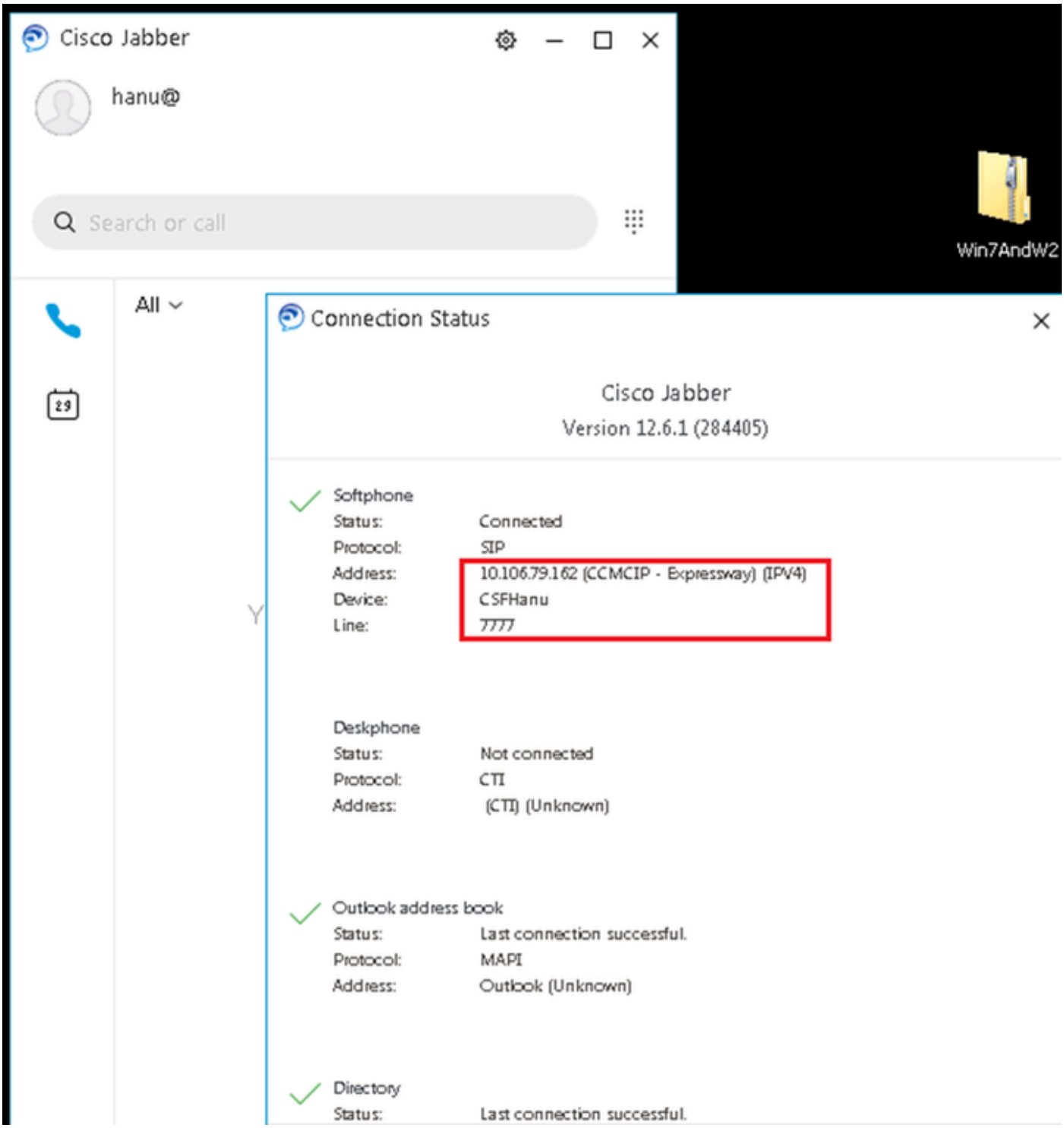


统一通信MRA区域状态为活动：

- Expressway-Core客户端证书具有服务器EKU和客户端EKU。
- Expressway核心服务器证书只有服务器EKU。



MRA客户端登录并注册：

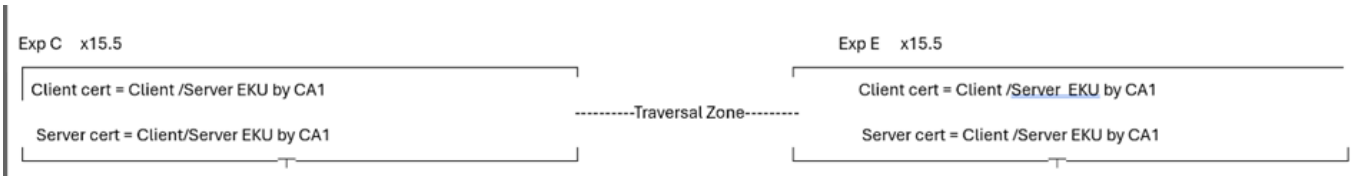


注意：比较并注意MRA和WebRTC代理要运行的证书中的EKU。它是工作部署和非工作部署的对比。

条件3:使用专用CA签署所有证书

CA 1 =内部CA

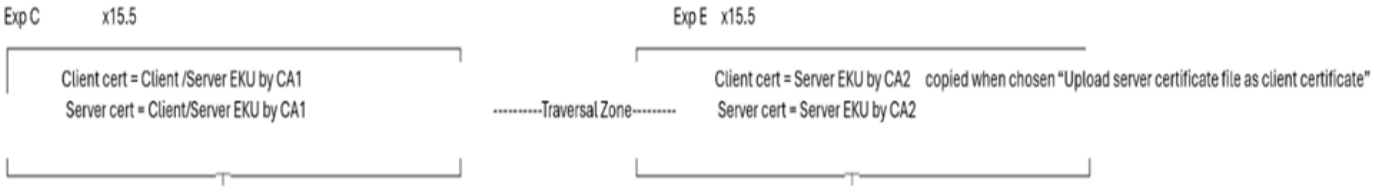
CA 2 =公共CA



在条件3中，所有证书由内部CA(CA1)签名。

- 当Expressway-E发出TLS连接时，CA 1根/中间需要与远端实体交换。如果远端没有功能或不允许上传专用CA证书，则TLS连接将失败。
- 如果私有证书不在OS信任存储中，MRA客户端将获得证书以接受弹出窗口。

条件4:Expressway边缘具有仅包含服务器EKU的公用证书



在条件4中，Expressway核心客户端和服务器证书是(CA1)内部CA签名，并且客户端和服务器EKU都存在。Expressway E服务器证书是公共CA签名，并且只有服务器EKU。服务器证书复制到客户端证书存储区，选择上传服务器证书文件作为客户端证书。

在条件4中，当与远端建立TLS连接时，如果Expressway -E发送TLS客户端hello，远端必须禁用客户端EKU检查（因为客户端证书没有客户端身份验证EKU），否则TLS连接不成功。

根据用户部署和使用案例，在现场可以有更多的条件或情景，但是由于我的思路有限，无法涵盖所有情况。但是，需要记住的要点是：

- #如果Expressway在TLS握手期间成为客户端，则客户端证书会呈现给对等体。
- #IF Expressway在TLS握手期间成为服务器；服务器证书显示给对等体。

这个推理已经和这些测试案例一起建立起来了。

场景 1

对于此场景，Expressway会在与Webex进行MTLS握手期间提供客户端证书。

Webex会议的视频呼叫：

呼叫流Jabber -à CUCM -à Exp Core —à Exp Edge —à Webex示例

10.106.80.31= Expressway边缘

163.129.37.33 = Webex

2026-03-24T11:54:26.106+00:00 smartslave tvcs:UTCTime="2026-03-24 11:54:26,106" Module="network.sip" Level="DEBUG": Action="Sent" Local-ip="10.106.80.31" Local-port="25002" Dst-ip="163.129.37.33" Dst-port="5061"

Expressway Edge具有使用此序列号(2f0000004c869c77c8981becde00000000004c)的客户端证书。

Expressway Edge在TLS协商期间向“Webex”发送客户端hello，然后发送客户端证书。

序列号2f0000004c869c77c8981becde00000000004c:

1. Expressway Edge在mTLS协商期间向“Webex”发送客户端hello(pkt= 13699)。

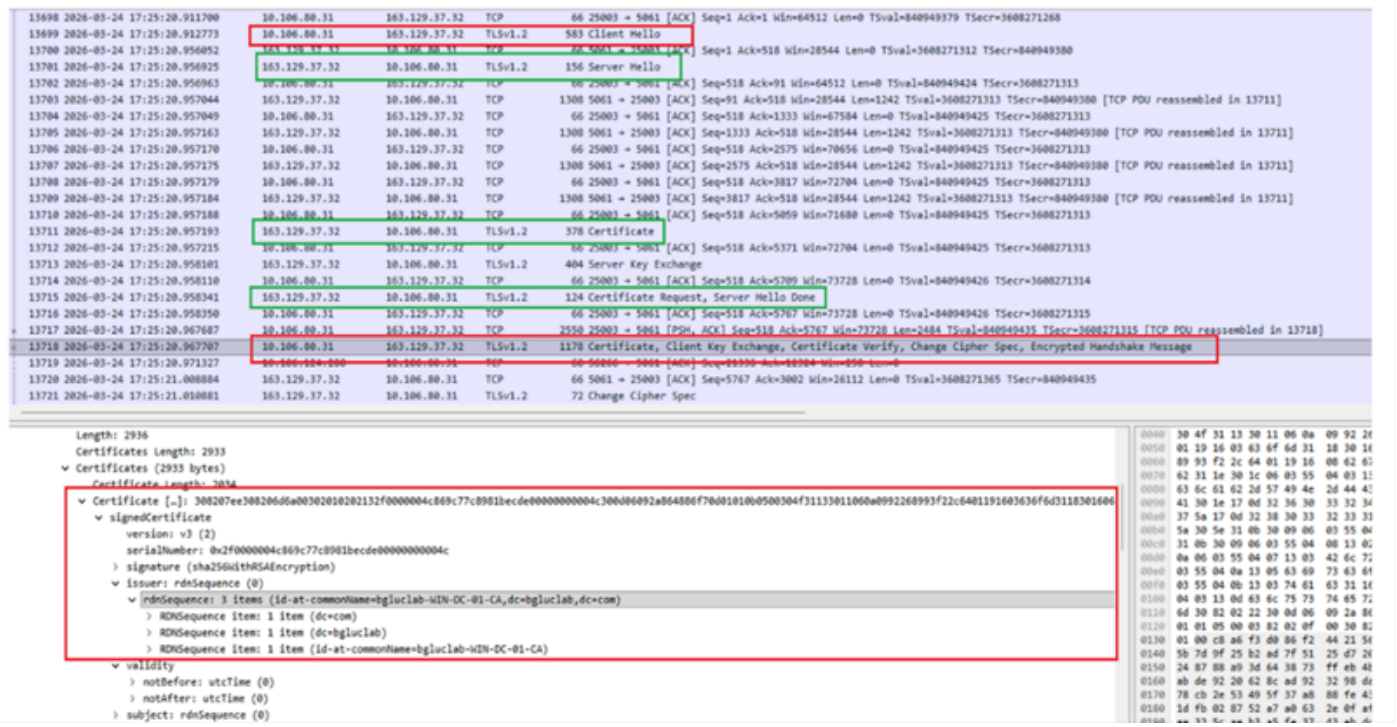
2. Webex向Expressway Edge(pkt=13701)发送服务器hello。

3. Webex将其证书发送到Expressway Edge(pkt=13711)。

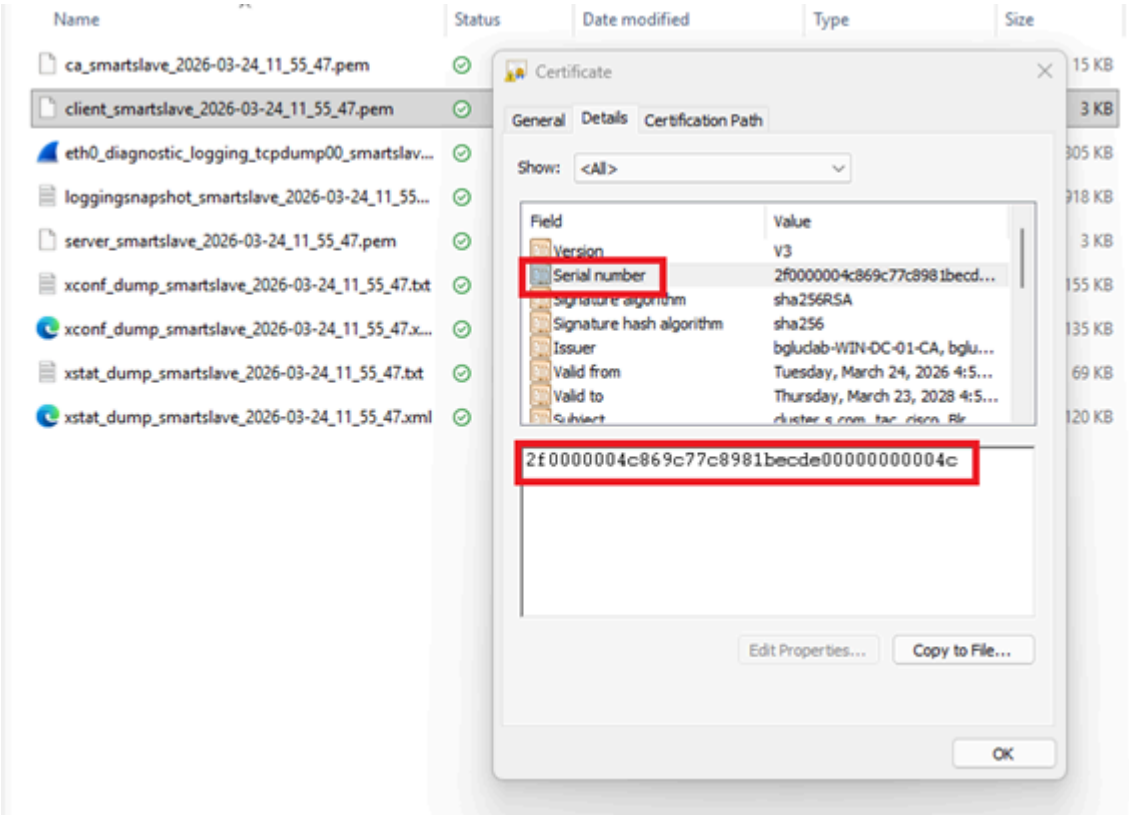
4. Webex请求Expressway边缘证书“CertificateRequest”(pkt=13715)。

5. Expressway Edge将其证书发送到Webex(pkt=13718)。

(屏幕截图)



来自Expressway边缘的客户端证书：



场景 2

Expressway在mTLS握手期间成为服务器实体，并显示其服务器证书：

在Expressway提供服务器证书的情况下，Expressway在5061上有一个安全邻居区域，其验证名称为ON。

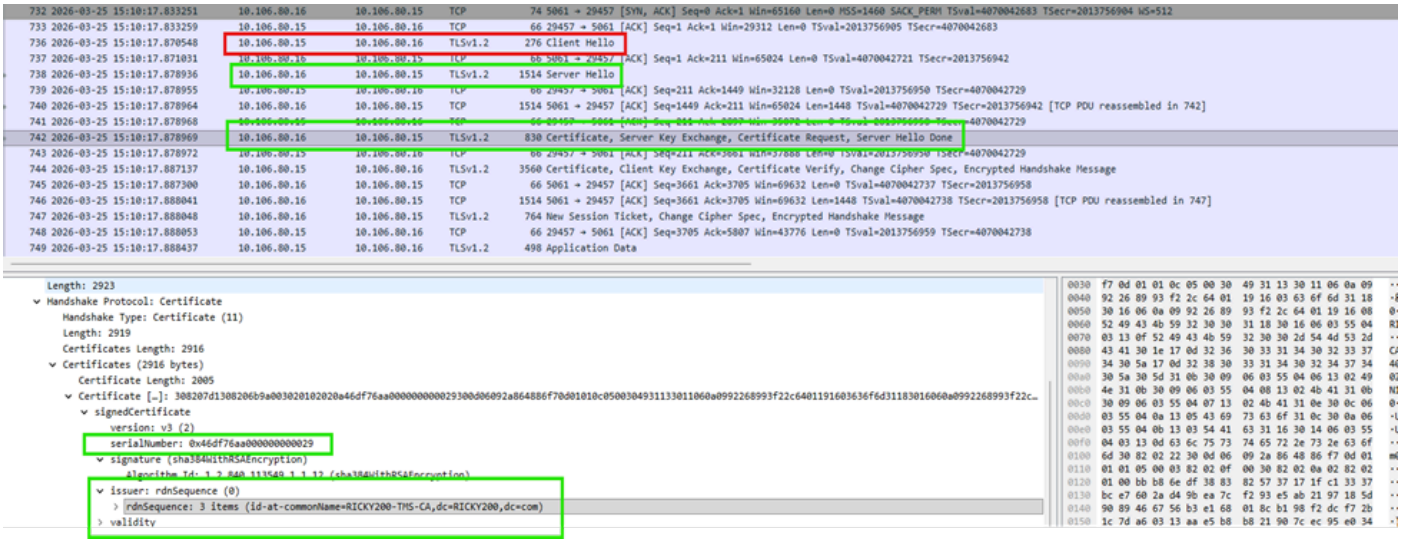
Expressway节点x15.5和Expressway节点x8.11.4之间的安全邻居区域：

10.106.80.15 (x8.11.4) sends a client hello to 10.106.80.16 (x15.5) (pkt=736)

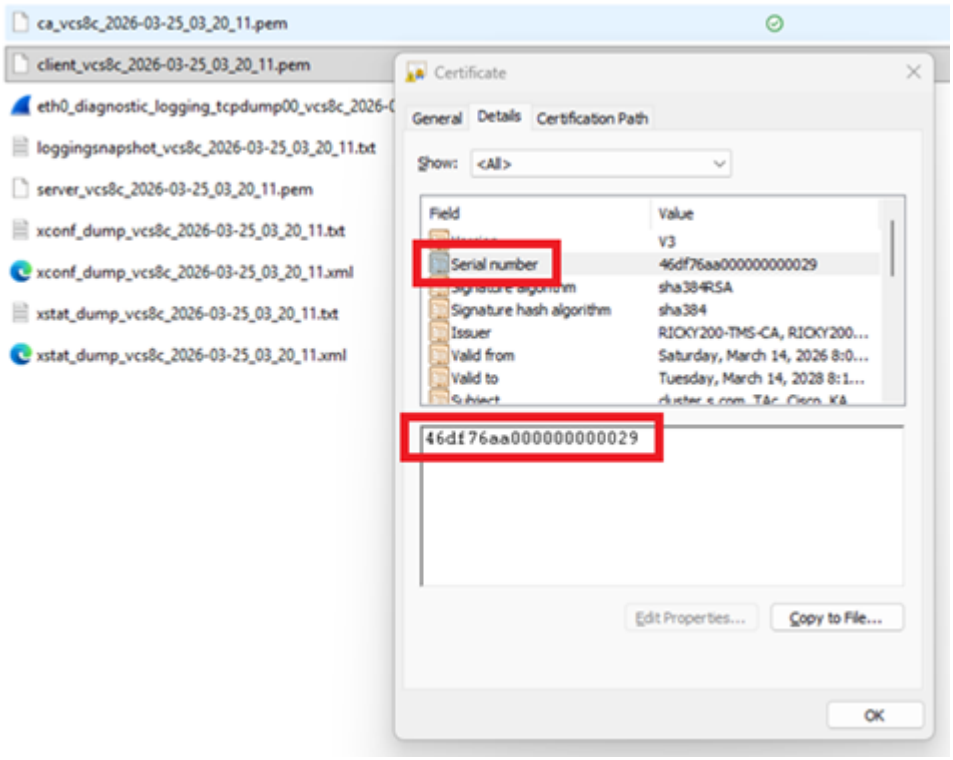
10.106.80.16 sends a server hello to 10.106.80.15 (pkt=738)

10.106.80.16 (x15.5) presents its server cert during TLS handshake (pkt=742) and requests client's cert

10.106.80.15 (x8.11.4) sends client certificate (pkt=744)



此屏幕截图显示序列号匹配的服务器证书：

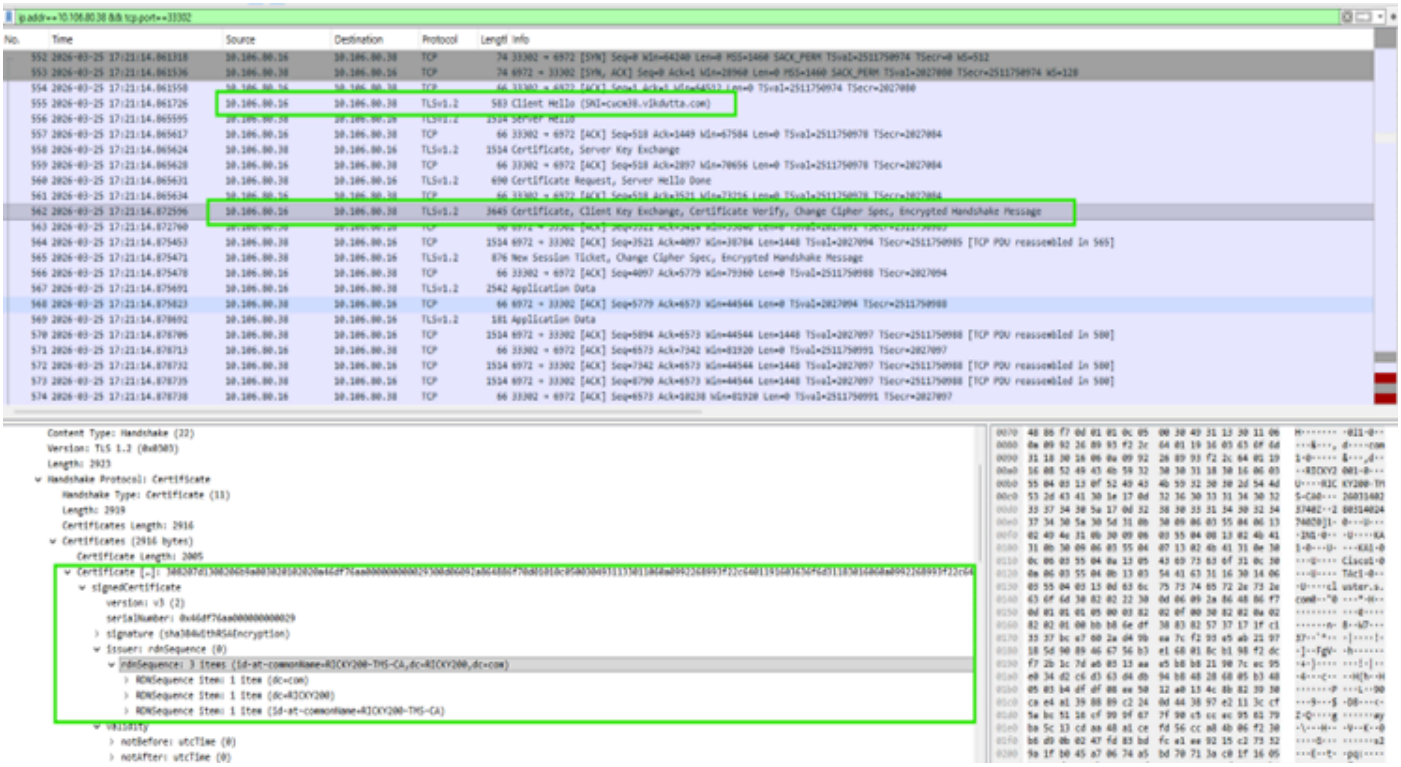


测试案例3:MRA客户端调配用于登录，工作流程包括Expressway核心和CUCM之间的流量服务器证书验证。

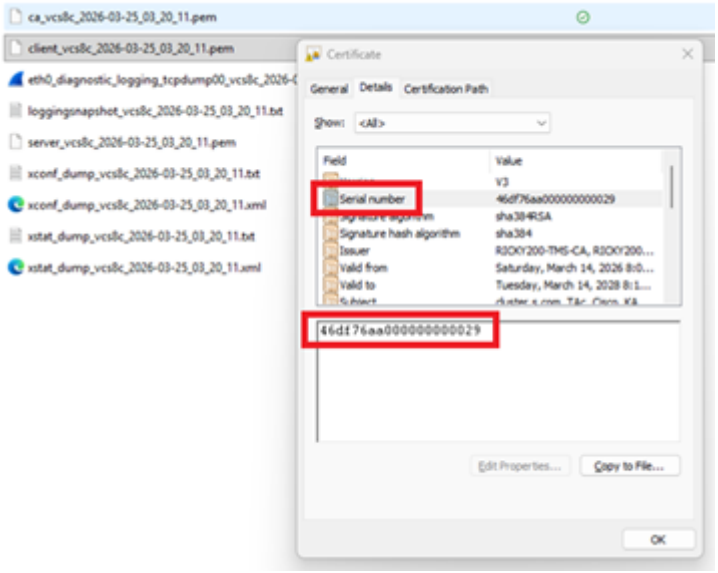
10.106.80.16 = Expressway核心x15.5

10.106.80.38 = CUCM

- Exp C 16在6972 TFTP上发送客户端hello。
- Exp C 16在TLS握手期间发送客户端证书。



Expressway核心客户端证书：



关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。